517,428

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 décembre 2003 (24.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/107585 A1

(51) Classification internationale des brevets[7] : H04L 9/08, H04N 7/16

(21) Numéro de la demande internationale : PCT/IB03/02425

(22) Date de dépôt international : 10 juin 2003 (10.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1002/02 12 juin 2002 (12.06.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRACARD SA [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : BRIQUE, Olivier [CH/CH]; Chemin de la Perrause 39, CH-1052 Le Mont-sur-Lausanne (CH). NICOLAS, Christophe [CH/CH]; Rue de Lausanne 59, CH-1028 Préverenges (CH). SASSELLI, Marco [CH/CH]; Chemin des Roches 20, CH-1803 Chardonne (CH).

(74) Mandataire : LEMAN CONSULTING SA; Route de Clémenty 62, CH-1260 Nyon (CH).

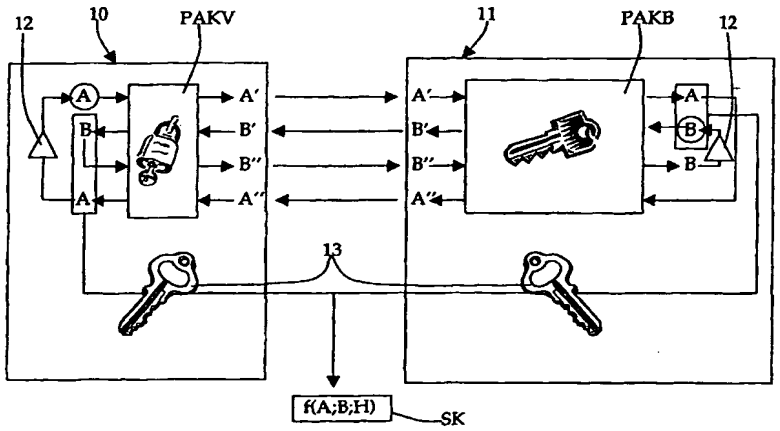
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet

[Suite sur la page suivante]

(54) Title: METHOD FOR SECURE DATA EXCHANGE BETWEEN TWO DEVICES

(54) Titre : PROCÉDÉ D'ÉCHANGE SÉCURISÉ D'INFORMATIONS ENTRE DEUX DISPOSITIFS



PAKB...PUBLIC KEY
PAKV...PRIVATE KEY
SK...SESSION KEY(I)

(57) Abstract: The invention concerns a method for secure data exchange between two locally interconnected devices. In a preferred embodiment, the first device (10) is a security module containing a first encryption key, called private key (PAKV) of a pair of asymmetric encryption keys. The second device is a receiver (11) comprising at least a second encryption key, called public key (PAKB) of said pair of asymmetric encryption keys. Each of the devices further comprises a symmetric key (13). The first device (10) generates a first random number (A) which is encrypted by means of the private key (PAKV), then transmitted to the second device (11), wherein it is decrypted by means of the public key (PAKB). The second device (11) generates a second random number (B) which is encrypted by means of said public key (PAKB), then transmitted to the first device (10), wherein it is decrypted by means of the private key (PAKV). A session key (SK), used for secure data exchanges, is generated by a combination of the symmetric key and the random numbers (A, B) generated and received by each of the devices.

[Suite sur la page suivante]

WO 03/107585 A1

eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : La présente invention concerne un procédé d'échange sécurisé d'informations entre deux dispositifs localement connectés entre eux.Dans un mode de réalisation préféré, le premier dispositif (10) est un module de sécurité contenant une première clé de chiffrement, dite clé privée (PAKV) d'une paire de clés de chiffrement asymétriques. Le second dispositif est un récepteur (11) comportant au moins une seconde clé de chiffrement, dite clé publique (PAKB) de ladite paire de clés de chiffrement asymétriques. Chacun des dispositifs comporte en outre une clé symétrique (13). Le premier dispositif (10) génère un premier nombre aléatoire (A) qui est chiffré par ladite clé privée (PAKV), puis transmis au second dispositif (11), dans lequel il est déchiffré au moyen de la clé publique (PAKB). Le second dispositif (11) génère un second nombre aléatoire (B) qui est chiffré par ladite clé publique (PAKB), puis transmis au premier dispositif (10), dans lequel il est déchiffré au moyen de la clé privée (PAKV). Une clé de session (SK), utilisée pour les échanges sécurisés d'informations, est générée par une combinaison de la clé symétrique (13) et des nombres aléatoires (A, B) générés et reçus par chacun des dispositifs.